



U.S. Department of Justice

Executive Office for United States Attorneys

Office of the Director


Room 2261, RFK Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530

(202) 514-2121

MEMORANDUM - Sent via Electronic Mail

DATE: **AUG 12 2009**

TO: ALL CONTRACTING OFFICERS
ALL ADMINISTRATIVE OFFICERS
ALL DISTRICT OFFICE SECURITY MANAGERS
ALL FIRST ASSISTANT UNITED STATES ATTORNEYS

From: 
Paul W. Suddes
Acting Chief Operating Officer

SUBJECT: Contractor Security of Systems and Data, Including Personally Identifiable Information

During the past year my staff has been grappling with issues involving data security. As you may recall, we were notified by the Procurement Executive that we are now required to include specific language in existing and new contracts that address data security. In addition, losses of equipment containing sensitive and personally identifiable information (PII) have been increasingly damaging to the citizens of the United States and the Department. After much discussion on the effect this may have on our ability to secure services and the possible financial impact, we have determined that we must implement the use of these clauses in existing and future contracts.

The "Security of Systems and Data, Including Personally Identifiable Data" clause addresses Department systems and data, including provisions governing the use of laptops by contractors. The clause is required to be inserted into all current and future contracts where a contractor handles data that originated within the Department, data that the contractor manages or acquires for the Department and/or data that is acquired in order to perform the contract and concerns Department programs or personnel.

The "Information Resellers or Data Brokers" clause must be used in contracts involving personally identifiable information obtained by the Department from a contractor, such as an information reseller or data broker (two examples of information resellers/data brokers are ChoicePoint, Inc. and Lexis-Nexis).

It is essential that all new applicable contracts include the appropriate security clause(s). Existing contracts should be modified to include the clause(s) if applicable. The clause(s) should be inserted in Statements of Work, Requests for Quotations, Requests for Proposals and made part of award documents. As a practical matter, Contracting Officers and COTRs should ensure that contractors are

aware of and understand the security requirements in these clauses. District Office Security Managers (DOSMs) and COTRs should ensure that contractors are in compliance with all aspects of the security clause(s). Contractors found not in compliance must immediately be brought to the attention of the Contracting Officer.

We realize that your office may face challenges in the use of these clauses. Specific technical questions pertaining to the security standards called out in the clause(s) should be addressed to the EOUSA Security Programs Staff or Information Systems Security Staff. Questions regarding contractual issues should be addressed to Wolfgang Nickle, Chief of Policy, Acquisitions Staff.

I understand that these are complicated changes for the United States Attorneys and vendor communities. I appreciate your cooperation and we will work with you to help implement these changes.

Attached please find the referenced clauses:

1. Security of Systems and Data, Including Personally Identifiable Data Clause.
2. Information Resellers or Data Brokers Clause.

Attachments

Information Resellers or Data Brokers

Under this contract, the Department obtains personally identifiable information about individuals from the contractor. The contractor hereby certifies that it has a security policy in place which contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, lost or acquired by an unauthorized person while the data is under the control of the contractor. In any case in which the data that was lost or improperly acquired reflects or consists of data that originated with the Department, or reflects sensitive law enforcement or national security interest in the data, the contractor shall notify the Department contracting officer so that the Department may determine whether notification would impede a law enforcement investigation or jeopardize national security. In such cases, the contractor shall not notify the individuals until it receives further instruction from the Department.

Security of Systems and Data, Including Personally Identifiable Data.

a. Systems Security

The work to be performed under this contract requires the handling of data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel.

For all systems handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 2640.2F. The contractor shall provide DOJ access to and information regarding the contractor's systems when requested by the Department in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, FISMA data reviews, and access by the DOJ Office of the Inspector General for its reviews.

The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the contracting officer (CO) certifying the following requirements:

1. Laptops must employ hard drive encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 validated product;
2. The contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
3. Mobile computing devices will utilize anti-viral software and a host-based firewall mechanism.
4. The contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is sensitive information unless designated as non-sensitive by the Department.
5. Contractor-owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, shall not be removed from DOJ facilities unless encrypted using a NIST FIPS 140-2 validated product;

6. When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;
7. Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;
8. Rules of behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and personally identifiable information;
9. All DOJ data will be removed from contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractor's project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work.

b. Data Security

By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified in paragraph a, in the event of any actual or suspected breach of such data (*i.e.*, loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately (and in no event later than within one hour of discovery) report the breach to the DOJ CO and the contracting officer's technical representative (COTR).

If the data breach occurs outside of regular business hours and/or neither the CO nor the COTR can be reached, the contractor shall call the EOUSA Security Operations Center at (803) 705-5533 within one hour of discovery of the breach. The contractor shall also notify the CO as soon as possible during regular business hours.

c. Personally Identifiable Information Notification Requirement

The contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department, and shall not proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the Department. The contractor assumes full responsibility for taking corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.

d. Pass-through of Security Requirements to Subcontractors

The requirements set forth in Paragraphs a through c, above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the contractor.